The spam filtering service provided with all hosted email is called Mail Scanner. MailScanner is a highly respected open source email security system. It is used at over 30,000 sites around the world, protecting top government departments, commercial corporations and educational institutions. This technology has fast become the standard email solution at many ISP sites for virus protection and spam filtering.

MailScanner scans email for viruses, spam, phishing, malware, and other attacks. By being open source, the technology in MailScanner has been reviewed many times over by some of the best and brightest in the field of computer security from around the world. MailScanner supports a wide range of virus scanners. Spam detection is accomplished via Spamassassin, which is by far the most popular and standardized spam detection engine.

MailScanner is considered an extremely stable and reliable product. Development continues, but is now in a stage of refinement and maintenance versus continual change.

cPanel MailScanner Configuration

MailScanner assigns a score to each email based on various attributes and triggers. The higher the score, the more likely the mail is to be spam. There are two levels of spam, low scoring and high scoring. High scoring spam is almost certainly spam, and low scoring spam is probably spam but it's possible to have false positives. The low scoring spam will have a score of at least 5 but less than 18. High scoring spam is email that has a score of at least 18. You can change these scores for your domain. The system default is to tag and deliver low scoring spam (5-18) and to delete high scoring spam (>18). You can customize that for your domain as well.

With the MailScanner service you can control what happens to spam and viruses by changing the configuration in your cPanel control panel. To access the MailScanner configuration options, login to your cPanel account and click on "MailScanner" in the Email section.

On the main MailScanner configuration page, if you have only one domain in your cPanel account you will see two main sections, ‘Current Settings’ and ‘Change Individual Domain Settings’. If you have more than one domain, you will see an additional section entitled ‘Change All Domain Settings’.

‘Currents Settings’ shows your current configuration. Changes can be made in ‘Email Black/Whitelist settings’, ‘Other settings’ and ‘Change Individual/All Domain Settings’. Each section is explained below.

Change Individual/All Domains Settings

- **Spam Scanning** - If you would like all your email for this domain scanned for spam, select yes. If you don't want your mail scanned for spam, select no. Default is yes
- **Virus Scanning** - If you would like all your email for this domain to be scanned for viruses, select yes. If you don't want your email scanned for viruses, select no. Default is yes
- D**eliver Cleaned Email**s - Most email viruses are sent by infected "zombie PCs" and have no valid content. If you want to receive notifications of each virus that was sent to you, select yes. If you do not want to receive these notifications, select no. Default is no

The next section allows you to **select the actions for the spam categories** Low & High Scoring Spam: Deliver (default for low scoring), Delete (default for high scoring) or Deliver to a specified address. Use the drop-down arrow to make changes.

Blacklist and Whitelist Settings

• **Spam whitelist** - You can add email addresses or domains to this list that you never want marked as spam. Please note that emails sent to you from these email addresses or domains will still be scanned for viruses and dangerous file attachments but they will not be marked as spam. Do not add your own domain to this list, as it will whitelist all emails sent TO your domain as well as FROM your domain.

• **Spam blacklist** - You can add to this list any email addresses or domains that you want always marked as high scoring spam. The action you have specified for High Scoring Spam in the Mail scanning options will be applied to any emails sent from domains or addresses on this list (i.e. tagged and delivered, deleted - the default, or forwarded).

Both lists allow up to 40 entries. One entry per line in the following formats: name@domain.com, *@domain.com, *@*.ru, or IP, or CIDR.

Other Settings

• **Low scoring spam setting** - You can change the level at which MailScanner will identify an email as low-scoring spam (probably spam) by changing this setting. If you change it to a higher number, you may receive more spams that have not been identified as spam by MailScanner. If you change it to a lower number you may find that MailScanner is identifying non-spam emails as spam, i.e. there will be more false-positives.

• **High scoring spam setting** - You can change the level at which MailScanner will identify an email as high scoring spam (almost certainly spam) by changing this setting. The default is 20 which we feel most customers will likely lower over time. If you find you are getting excessive amounts of low scoring spam with a score just below 20, you may want to change this setting to a smaller number. Since high scoring spam is deleted, we recommend not making changes to this setting for a couple weeks. When you do change either threshold, we suggest changing it by 1 number a week to avoid potentially missing legitimate emails.

• **Additional email address to list for forwarding spam** - If you'd like to have spam forwarded to a specific email address, for instance an email address on another domain, you can specify that email address here. It will then be listed as one of the options for Low and High Scoring Spam in the Mail Scanning Options so you can select it. If you choose to have the spam forwarded to an alternate email address you must create this email address in cPanel. We suggest creating and using "spam@yourdomain.com". You can create and add more than 1 address.

MailScanner Frequently Asked Questions

• Will spam be deleted before I retrieve my email?

By default, our servers delete high scoring spam (20 or above). While you can change this, we have found that at least 40% of all inbound email (and at times as much as 70%) is spam and opted to have that dropped. Any lower scoring email reported by the system as spam will have the subject line modified and header records added (tagged) to indicate possible spam. That “tag” allows you to filter the message from your inbox into a separate folder so that you can check them later. You can configure MailScanner to delete email marked as Spam and/or Definitely Spam for you, but beware of the issues in the following answers to spam related questions.

• Should I tell you about incorrectly tagged spam?

Not unless it is an email from someone you regularly receive email from. The simplest thing to do would be to add an extra inbox rule in your email client to keep email from them in your inbox. Alternatively, you can add them to your whitelist in the cPanel MailScanner configuration.

- **Will all spam be detected?**

No. Some spam will occasionally come through untagged. All the email is scanned and assigned a score based on the likelihood that an email is spam. Thresholds (low scoring and high scoring spam) are used to determine whether an email should be tagged as spam. This is done to help avoid false-positives and false-negatives.

- **Is all email tagged as spam, actually spam?**

Not necessarily. The system is not foolproof and there will be instances where legitimate email is tagged as spam or where spam is not tagged. Therefore, all middle scoring email is delivered by default. You can filter the email in your email client and check through the spam to ensure there is no email that you need.

- **Will viruses be deleted before I retrieve my email?**

Yes, if you set Virus Scanning to yes in the MailScanner Front-end. All emails and file attachments will be scanned for viruses. If one is found, the virus is removed from the email before it is delivered to your mailbox, a text file attachment will be added to the email notifying you of the virus infection. Removed viruses and dangerous file attachments removed from email may be stored in a quarantine area on the server for 30 days. You can request the file from quarantine as described in the text file attachments, or, preferably ask the sender to resend the file in a zip archive.

- **Will all viruses be detected?**

No system can guarantee 100% detection, though nearly all infected files and dangerous file attachments should be detected using this service. The service scans all email received and sent through the server to help ensure that you do not accidentally start spreading a virus yourself.

- **Do I still need a virus scanner on my computer?**

Absolutely! Not only can the service not guarantee that all email viruses will be detected, there are many other ways that your computer can become infected. You should always install an anti-virus solution on every computer and ensure that it is constantly kept up to date.

- **How do I know whether and email has a virus or is a spam?**

There are two methods used to identify these emails to you: a subject line prefix and an additional email header.
First, the subject line of the affected email will be prefixed with one of the following. The bold headings are recommended for use in your email client filters:

  - **{Disarmed}** - indicates that the email contained html tags that are considered dangerous, e.g. iframe and form tags
  - **{Virus?}** - indicates that the email contained a virus and has had the attachment removed.
  - **{Filename?}** - indicates that the email contained a dangerous file attachment which has been removed.

◦ **{Spam?}** - indicates that the email is likely to be spam - you should filter these emails into a separate folder in your email client.
◦ **{Definitely Spam?}** - indicates that the email is almost definitely spam because it got a very high detection score. Nearly all of these will be deleted before they reach your inbox.

Second, additional headers are added to the email:
◦ X-_____-VirusCheck: Found to be clean - indicates that the email passed the virus scanning tests.
◦ X-_____-VirusCheck: Found to be infected - indicates that email contained a virus which has been removed.
◦ X-_____-SpamCheck: spam - indicates that the email is likely to be spam and contains information on how the score was reached.
◦ X-_____-SpamScore: ssssss - indicates the spam score for the email. Each s represents 1 point, so sssss indicates a score of 5. The service has a default threshold of 5 for {Spam?} and 20 for {Definitely Spam?}

• **Can the system simply delete all email marked as spam?**

We advise against this as it is possible that legitimate email will be deleted and the sender will never know that you didn't receive it. We recommend filtering the email in your email client and placing it in a separate folder so that you can check through it in your own time.

If you're happy that email marked as {Spam?}, and/or more suitably {Definitely Spam?} you can then configure MailScanner to delete that email by lowering the High Scoring threshold.

Another alternative is to have all email marked as {Spam?}, and/or more suitably {Definitely Spam?} delivered to a specific email address. For example, spam@mydomain.com.

• **How do I configure my email software to filter spam into a separate folder?**

You should create a separate folder in your email client called Spam. Then create an inbox rule to place any email containing the strings {Spam?} or {Definitely Spam?} into that folder.

• **What can I do to prevent receiving spam?**

Have a look at the self-help checklist below.

Spam Self-Help

Here are some things you can do to help prevent receiving spam in the first place:

• Do not use a catchall email account on your domain(s). Only list aliases and POP accounts that you actually use. This stops the frequent spams that fire off emails to a list of names on a domain.

• Obfuscate your email addresses on your website, i.e. replace them with JavaScript "trick" email addresses, or switch to web forms for initial contact, rather than displaying an email address.

• Never, ever, click on any links in any spam - especially not to "unsubscribe". All this does is confirm to the spammer that they have a "live" address.

• Configure your client to read any incoming emails in plain-text, never html. Html spam emails contain links to graphics and scripts on spammers sites, confirming your email address.

A simple web search on “how to stop spam emails” will also yield many additional suggestions.

MailScanner Dangerous File Attachments

The following is a list of file attachments that are blocked by the service (the attachments are removed from emails before delivery to you and placed in a quarantine area for 30 days should you wish to receive them):

These are known to be dangerous in almost all cases:

.reg - Possible Windows registry attack
.chm - Possible compiled Help file-based virus
.cnf - Possible SpeedDial attack
.hta - Possible Microsoft HTML archive attack
.ins - Possible Microsoft Internet Comm. Settings attack
.jse_ - Possible Microsoft JScript attack
.lnk - Possible Eudora *.lnk security hole attack
.ma_ - Possible Microsoft Access Shortcut attack
.pif - Possible MS-Dos program shortcut attack
.scf - Possible Windows Explorer Command attack
.sct - Possible Microsoft Windows Script Component attack
.shb - Possible document shortcut attack
.shs - Possible Shell Scrap Object attack
.vbe .vbs - Possible Microsoft Visual Basic script attack
.wsc .wsf .wsh - Possible Microsoft Windows Script Host attack
.xnk - Possible Microsoft Exchange Shortcut attack

These 2 added by popular demand - Very often used by viruses:

.com - Windows/DOS Executable
.exe - Windows/DOS Executable

These are very dangerous and have been used to hide viruses:

.scr - Possible virus hidden in a screensaver
.bat - Possible malicious batch file script
.cmd - Possible malicious batch file script
.cpl - Possible malicious control panel item
.mhtml - Possible Eudora meta-refresh attack

Deny filenames ending with CLSID's
{[a-hA-H0-9-]{25,}\} Filename trying to hide its real extension
Examples:
A977FF0C-8757-4E76-8533-482F91946233
000209FF-0000-0000-C000-000000000046

Deny filenames with lots of contiguous white space in them.
'Filename contains lots of white space'

Deny all other double file extensions. This catches any hidden filenames.
'Found possible filename hiding' Examples:

.txt.pif .doc.com
.doc.pif .txt.exe